RECEIVED
OCT 17 2017
UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF MISSISSIPPI

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF MISSISSIPPI

BERONICA JONES and MICHAEL SAUCIER, on behalf of themselves and all others similarly situated,	)	**CLASS ACTION**
Plaintiffs,	)	**No.** 3:17-CV-211-SA-JMV
v.	)	**JURY TRIAL DEMANDED**
EQUIFAX INC., and EQUIFAX INFORMATION SERVICES, LLC	)	
Defendants.	)	

CLASS ACTION COMPLAINT

Plaintiffs Beronica Jones and Michael Saucier ("Plaintiffs" or "Class Representatives"), on behalf of themselves and the Class and Subclass defined below, allege the following against Equifax Inc., and Equifax Information Services, LLC ("Defendants," "Equifax," or the "Company"), based on personal knowledge as to Plaintiffs' conduct and on information and belief as to the acts of others.*

I. INTRODUCTION

1. Defendants Equifax Inc. and Equifax Information Services, LLC operate "Equifax," one of the three largest consumer credit reporting agencies in the United States.

* Unless otherwise indicated "Equifax" denotes both Equifax defendants.

Plaintiffs have been consumers of Equifax's services and entrusted Defendants with their personal information. They bring this action on a class basis alleging violations of the federal Fair Credit Reporting Act, as well as common law claims for negligence, negligence per se, breach of implied contract, unjust enrichment, invasion of privacy, and bailment. Plaintiffs seek declaratory and injunctive relief and redress for affected Equifax consumers.

2. Because Plaintiffs and the Class entrusted Defendants with their sensitive personal information, Equifax owed them a duty of care to take adequate measures to protect the information entrusted to it, to detect and stop data breaches, and to inform Plaintiffs and the Class of data breaches that could expose Plaintiffs and the Class to harm. Equifax failed to do so.

3. Equifax acknowledges that, between May 2017 and July 2017, it was the subject of a data breach in which unauthorized individuals accessed Equifax's database and the names, Social Security numbers, addresses, and other Personal Identifying Information ("PII") stored therein (hereinafter the "Data Breach"). According to Equifax, the Data Breach affected as many as 143 million people. Equifax admits that it discovered the unauthorized access on July 29, 2017, but failed to alert Plaintiffs and the Class to the fact of the breach until September 7, 2017.

4. The Data Breach was the inevitable result of Equifax's inadequate approach to data security and the protection of the PII that it collected during the course of its business. Defendants knew and should have known of the inadequacy of their own data security. Equifax has experienced similar such breaches of PII on smaller scales in the past, including in 2013, 2016, and even as recently as January 2017. Over the years, Equifax has jeopardized the PII and, as a result, financial information of hundreds of thousands of Americans.

5. Despite this long history of breaches, Defendants have failed to prevent the Data

Breach that has exposed the personal information of over 100 million Americans. The damage done to these individuals may follow them for the rest of their lives, as they will have to monitor closely their financial accounts to detect any fraudulent activity and incur out-of-pocket expenses for years to protect themselves from, and to combat, identity theft now and in the future.

6. Equifax knew and should have known the risks associated with inadequate security, and with delayed reporting of the breach. The potential for harm caused by insufficient safeguarding of PII is profound. With data such as that leaked in the Data Breach, identity thieves can cause irreparable and long-lasting damage to individuals, from filing for loans and opening fraudulent bank accounts to selling valuable PII to the highest bidder.

7. In the case of Defendants' Data Breach, the potential repercussions for consumers are particularly egregious. Privacy researchers and fraud analysts have called this attack "as bad as it gets." "On a scale of 1 to 10 in terms of risk to consumers," it is a 10.[1]

8. Defendants failed to inform millions of consumers of the Data Breach until September 7, 2017, over a month after Defendants first discovered it on July 29. While Defendants took no steps at that time to inform the public in the interim, Defendants did not hesitate to protect themselves; at least three Equifax senior executives, including CFO John Gamble, upon information and belief, sold shares worth $1.8 million in the days following the Data Breach.[2]

9. To provide relief to the millions of people whose PII has been compromised by the Data Breach, Plaintiffs bring this action on behalf of themselves and all others similarly

---

[1] https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html

[2] https://www.bloomberg.com/news/articles/2017-09-07/three-equifax-executives-sold-stock-before-revealing-cyber-hack

situated. They seek to recover actual and statutory damages, equitable relief, restitution, reimbursement of out-of-pocket losses, other compensatory damages, credit monitoring services with accompanying identity theft insurance, and injunctive relief including an order requiring Equifax to improve its data security and bring to an end its long history of breaches at the expense of consumers.

II. THE PARTIES

A. PLAINTIFFS

10. Plaintiff Beronica Jones is an individual consumer who resides in Sumner, Mississippi. Plaintiff engaged, or authorized the engagement of, Equifax at various times. As a result, Equifax has possessed Plaintiff's financial history, including her Social Security number, birthdate, personal addresses, and other sensitive personally identifying information. Plaintiff was a victim of the breach. Since the breach, she has spent time monitoring and attempting to protect her credit and accounts from the improper use of her PII obtained by unauthorized third parties as a result of the Data Breach.

11. Plaintiff Michael Saucier is an individual consumer who resides in Gulfport, Mississippi. Plaintiff engaged, or authorized the engagement of, Equifax at various times. As a result, Equifax has possessed Plaintiff's financial history, including his Social Security number, birthdate, personal addresses, and other sensitive personally identifying information. Plaintiff was a victim of the breach. Since the breach, he has spent time monitoring and attempting to protect his credit and accounts from the improper use of his PII obtained by unauthorized third parties as a result of the Data Breach.

B. DEFENDANTS

12. Defendant Equifax Inc. is a multi-billion dollar corporation formed under the laws of the State of Georgia with its corporate headquarters in Atlanta, GA. It provides credit information services to millions of businesses, governmental units, and consumers across the globe. Equifax operates through various subsidiaries and agents, each of which acted as agents of Equifax, or in the alternative, in concert with Equifax.

13. Defendant Equifax Information Services, LLC is a Georgia limited liability company with its principal place of business located in Atlanta, GA. Equifax Information Services, LLC is a subsidiary of Equifax, Inc., and is responsible for collecting and reporting consumer information to financial institutions.

III. JURISDICTION AND VENUE

14. This Court has jurisdiction under 28 U.S.C. § 1332 because there are over 100 Class Members, the amount in controversy exceeds $5 million exclusive of interest and costs, and this is a class action in which many members of the proposed classes, on the one hand, and Defendants, on the other, are citizens of different states.

15. The Northern District of Mississippi has personal jurisdiction over Defendants because Defendants do business in Mississippi and in this District; Defendants advertise in a variety of media throughout the United States, including Mississippi; and many of the acts complained of and giving rise to the claims alleged herein occurred in this District. Defendants intentionally avail themselves of the markets within this state to render the exercise of jurisdiction by this Court just and proper.

16. Venue is proper pursuant to 28 U.S.C. § 1391 because Defendants conduct substantial business in this District, a substantial part of the events and omissions giving rise to the claims alleged herein occurred in this District, and a substantial part of the property that is the

subject of the action is situated in this District.

IV. FACTUAL ALLEGATIONS

17. Equifax has collected and stored personal and credit information from Class Members, including Plaintiffs.

18. Equifax owed a duty to Plaintiffs and the Class, who entrusted Defendants with their private information, to use reasonable care to protect their PII from unauthorized access by third parties and to detect and stop data breaches, to comply with laws implemented to preserve the privacy of this information, and to promptly notify Plaintiffs and the members of the nationwide Class and Mississippi Subclass (defined *infra*) if their information was disclosed to an unauthorized third party.

19. Equifax knew or should have known that its failure to meet this duty would cause substantial harm to Plaintiffs and the Class, including serious risks of credit harm and identity theft for years to come.

20. As Equifax was well-aware, or reasonably should have been aware, the PII collected, maintained and stored in the POS systems is highly sensitive, susceptible to attack, and could be used for wrongful purposes by third parties, including identity theft and fraud. It is well known and the subject of many media reports that PII is highly coveted and a frequent target of hackers. Prior to May 2017, Equifax had experienced at least three major cybersecurity incidents in which consumers' personal information was compromised and accessed by unauthorized third parties.

21. Despite frequent public announcements of data breaches of corporate entities, including announcements made by Equifax itself, Equifax maintained an insufficient and inadequate system to protect the PII of Plaintiffs and Class Members, in breach of its duties to

Plaintiffs and the Class. Given the Company's history of cyberattacks and its reputation as an industry leader in data breach security, Equifax could have and should have invested more money and resources into ensuring the security of its data.

22. Because Equifax negligently failed to maintain adequate safeguards, unauthorized third parties managed to exploit a weakness in Equifax's U.S. website application to gain access to sensitive data for roughly two months, beginning in mid-May 2017. The information accessed included names, Social Security numbers, birth dates, addresses, and, in some cases, driver's license numbers. In addition, credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers, were accessed.

23. Equifax was, or reasonably should have been, aware of the specific vulnerability in its systems as early as March 2017. In or about March 2017, Equifax discovered a vulnerability in its U.S. website: Apache Struts CVE-2017-5638. Despite knowing that this system flaw jeopardized the PII of millions of consumers, Equifax failed to implement an effective patch for at least 9 weeks, and failed to check this known vulnerability regularly to ensure that consumers' information was secure throughout the period of the Data Breach.

24. The Equifax Data Breach was a direct and proximate result of Equifax's failure to properly safeguard and protect Plaintiffs' and Class Members' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Equifax's failure to establish and implement appropriate safeguards to ensure the security and confidentiality of Plaintiffs' and Class Members' PII to protect against reasonably foreseeable threats to the security or integrity of such information.

25. Equifax delayed informing Plaintiffs, the Class, and the public of the Data Breach. On September 7, 2017, Equifax announced to the public that it had discovered "unauthorized access" to company data, which jeopardized sensitive information for millions of its consumers.

26. As of this date, Equifax has yet to inform consumers whether their specific personal data was impacted by this massive security breach.

27. At all relevant times, Equifax knew, or reasonably should have known, of the importance of safeguarding PII and of the foreseeable consequences if its data security system was breached, including, specifically, the significant costs that would be imposed on individuals as a result of a breach.

28. As a direct, proximate, and foreseeable result of Equifax's failure to meet its duty of care, including by failing to maintain adequate security measures and failing to provide adequate notice of the Data Breach, Plaintiffs and the Class have suffered and will continue to suffer substantial harm, including inconvenience, distress, injury to their rights to the privacy of their information, increased risk of fraud, identity theft, and financial harm, the costs of monitoring their credit to detect incidences of this, and other losses consistent with the access of their PII by unauthorized sources.

29. Armed with the stolen information, unauthorized third parties now possess keys that unlock consumers' medical histories, bank accounts, employee accounts, and more. Abuse of sensitive credit and personal information can result in considerable harm to victims of security breaches. Criminals can take out loans, mortgage property, open financial accounts and credit cards in a victim's name, obtain government benefits, file fraudulent tax returns, obtain medical services, and provide false information to police during an arrest, all under the victim's name.

Furthermore, this valuable information can also be sold to others with similar nefarious intentions.

30. As a direct and proximate result of Equifax's wrongful actions and inaction and the resulting Data Breach, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands, and attempt instead to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports. This time has been lost forever and cannot be recaptured. In all manner of life in this country, time has constantly been recognized as compensable, for many consumers it is the way they are compensated, and even if retired from the work force, consumers should be free from having to deal with the consequences of a credit reporting agency's wrongful conduct, as is the case here.

31. A breach of this scale requires Plaintiffs and Class Members to incur the burden of scrupulously monitoring their financial accounts and credit histories to protect themselves against identity theft and other fraud and to spend time and incur out-of-pocket expenses to protect against such theft. This includes obtaining credit reports, enrolling in credit monitoring services, freezing lines of credit, and more. Where identity theft is detected, Plaintiffs and Class Members will incur the burden of correcting their financial records and attempting to correct fraud on their accounts, to the extent that that is even possible. Plaintiffs and Class Members will likely spend considerable effort and money for the rest of their lives on monitoring and responding to the repercussions of this cyberattack.

32. Equifax's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiffs' and Class Members' PII, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. theft of their personal and financial information;

b. unauthorized charges on their debit and credit card accounts;

c. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals and already misused via the sale of Plaintiffs' and Class Members' information on the black market;

d. the untimely and inadequate notification of the Data Breach;

e. the improper disclosure of their PII;

f. loss of privacy;

g. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

h. ascertainable losses in the form of deprivation of the value of their PII, for which there is a well-established national and international market;

i. ascertainable losses in the form of the loss of cash back or other benefits as a result of their inability to use certain accounts and cards affected by the Data Breach;

j. loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse credit notations; and,

k. the loss of productivity and value of their time spent attempting to ameliorate, mitigate and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all such issues resulting from the Data Breach.

33. Because Equifax has demonstrated an inability to prevent a breach or stop it from continuing even after the breach was detected, Plaintiffs and members of the Class have an undeniable interest in insuring that their PII, which remains in Equifax's possession, is secure, remains secure, is properly and promptly destroyed and is not subject to further theft.

V. CLASS ACTION ALLEGATIONS

34. Plaintiffs bring this action pursuant to Fed. R. Civ. P. 23 seeking injunctive and monetary relief for Equifax's systemic failure to safeguard personal information of Plaintiffs and Class Members.

A. CLASS DEFINITIONS

35. Plaintiffs seek relief in their individual capacities and as representatives of all others who are similarly situated.

36. The "Class" is defined as all persons residing in the United States whose personal data Equifax collected and stored and whose personal information was placed at risk and/or disclosed in the Data Breach affecting Equifax from May to July 2017.

37. The "Mississippi Subclass" is defined as all persons residing in Mississippi whose personal data Equifax collected and stored and whose personal information was placed at risk and/or disclosed in the Data Breach affecting Equifax from May to July 2017.

38. Excluded from either class are all attorneys for the class, officers, and members of Equifax, including officers and members of any entity with an ownership interest in Equifax, any judge who sits on this case, and all jurors and alternate jurors who sit on this case.

39. Except where otherwise noted, "Class Members" shall refer to members of the nationwide Class and the Mississippi Subclass collectively.

40. Plaintiffs hereby reserves the right to amend or modify the class definitions with greater specificity after having had an opportunity to conduct discovery.

B. REQUIREMENTS OF RULE 23(a)

i. Numerosity and Impracticability of Joinder

41. The proposed Class and Subclass are so numerous that joinder of all members is impracticable.

42. Upon information and belief, there are more than 143 million members of the proposed Nationwide Class, and many thousands of members in the Mississippi Subclass.

43. The Class Members are readily ascertainable. Equifax has access to information about the Data Breach, the time period of the Data Breach, and which individuals were affected. Using this information, the members of the Class can be identified and their contact information ascertained for purposes of providing notice.

ii. Common Questions of Law and Fact

44. Every Class Member suffered injuries as alleged in this complaint because of Defendants' misconduct. The prosecution of Plaintiffs' claims will require the adjudication of numerous questions of law and fact common to the Class. The common questions of law and fact predominate over any questions affecting only individual Class Members. The common questions include:

a. Whether Defendants engaged in the wrongful conduct alleged herein;

b. Whether Defendants owed a duty to Plaintiffs and Class Members to adequately protect their personal information;

c. Whether Defendants breached their duties to protect the personal information of Plaintiffs and Class Members;

d. Whether Defendants knew or should have known that Equifax's data security systems and processes were unreasonably vulnerable to attack;

e. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendants' conduct, including increased risk of identity theft and loss of value of personal information; and

f. Whether Plaintiffs and Class Members are entitled to equitable relief including injunctive relief.

iii. Typicality of Claims and Relief Sought

45. Plaintiffs have suffered the same violations and similar injuries as other Class Members arising out of and caused by Defendants' common course of conduct. All Class Members were subject to the same acts and omissions by Defendants, as alleged herein, resulting in the breach of personal information.

46. Plaintiffs possess and assert each of the claims on behalf of the proposed Class. They seek similar relief as other Class Members.

iv. Adequacy of Representation

47. Plaintiffs' interests are coextensive with those of the members of the proposed Class. Each suffered risk of loss and credit harm and identity theft caused by Equifax's wrongful conduct and negligent failure to safeguard their data, the injuries suffered by Plaintiffs and the Class Members are identical (i.e. the costs to monitor and repair their credit through a third-party service), and Plaintiffs' claims for relief are based upon the same legal theories as are the claims of the other Class Members. Plaintiffs are willing and able to represent the proposed Class fairly and vigorously.

48. Plaintiffs have retained counsel sufficiently qualified, experienced, and able to conduct this litigation and to meet the time and fiscal demands required to litigate a class action of this size and complexity.

C. REQUIREMENTS OF RULE 23(b)(2)

49. Equifax has acted or refused to act on grounds generally applicable to Plaintiffs and the proposed Class by failing to take necessary steps to safeguard Plaintiffs' and Class Members' personal information.

50. Equifax's systemic conduct justifies the requested injunctive and declaratory relief with respect to the Class.

51. Injunctive, declaratory, and affirmative relief are predominant forms of relief sought in this case. Entitlement to declaratory, injunctive, and affirmative relief flows directly and automatically from proof of Equifax's failure to safeguard consumers' personal information. In turn, entitlement to declaratory, injunctive, and affirmative relief forms the factual and legal

predicate for the monetary and non-monetary remedies for individual losses caused by Equifax's failure to secure such information.

D. REQUIREMENTS OF RULE 23(b)(3)

52. The resolution of this case is driven by the common questions set forth above. These questions, relating to Equifax's liability and the Class Members' entitlement to relief, are substantial and predominate over any individualized issues.

53. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. In fact, no other feasible methods exist. Individual Class Members have modest damages and lack the financial resources to vigorously prosecute a lawsuit against a large corporation such as Equifax.

54. Class action treatment will permit a large number of similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of efforts and expense that numerous individual actions engender.

55. The prosecution of separate actions by individual members of the Class would create a risk of inconsistent and/or varying adjudications with respect to the individual members of the Class, establishing incompatible standards of conduct for Defendants and resulting in the impairment of Class Members' rights and the disposition of their interests through actions to which they were not parties.

56. The issues in this class action can be decided by means of common, classwide proof. In addition, the Court can, and is empowered to, fashion methods to efficiently manage this action as a class action.

E. RULE 23(c)(4) ISSUE CERTIFICATION

57. Additionally, or in the alternative, the Court may grant "partial" or "issue" certification under Rule 23(c)(4). Resolution of common questions of fact and law would materially advance the litigation for all Class Members.

COUNT I

WILLFUL VIOLATION OF THE FEDERAL FAIR CREDIT REPORTING ACT

58. Plaintiffs incorporate paragraphs 1 through 57 by reference.

59. Plaintiffs and Class Members are consumers entitled to the protections of the Fair Credit Reporting Act, 15 U.S.C. § 1681a(c) ("FCRA").

60. Under the FCRA, a "consumer reporting agency" is defined as "any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties . . . ." 15 U.S.C. § 1681a(f).

61. Equifax is a consumer reporting agency under the FCRA because, for monetary fees, it regularly engages in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties.

62. As a consumer reporting agency, the FCRA requires Equifax to "maintain reasonable procedures designed to . . . limit the furnishing of consumer reports to the purposes listed under section 1681b of this title." 15 U.S.C. § 1681e(a).

63. Under the FCRA, a "consumer report" is defined as "any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's

credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for -- (A) credit . . . to be used primarily for personal, family, or household purposes; . . . or (C) any other purpose authorized under section 1681b of this title." 15 U.S.C. § 1681a(d)(1). The compromised data was a consumer report under the FCRA because it was a communication of information bearing on Class Members' credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living used, or expected to be used or collected in whole or in part, for the purpose of serving as a factor in establishing the Class Members' eligibility for credit.

64. As a consumer reporting agency, Equifax may only furnish a consumer report under the limited circumstances set forth in 15 U.S.C. § 1681b, "and no other." 15 U.S.C. § 1681b(a). None of the purposes listed under 15 U.S.C. § 1681b permit credit reporting agencies to furnish consumer reports to unauthorized or unknown entities, or computer hackers such as those who accessed the Class Members' PII. Equifax violated § 1681b by furnishing consumer reports to unauthorized or unknown entities or computer hackers, as detailed above.

65. Equifax furnished Class Members' consumer reports by disclosing their consumer reports to unauthorized entities and computer hackers; allowing unauthorized entities and computer hackers to access their consumer reports; knowingly and/or recklessly failing to take security measures that would prevent unauthorized entities or computer hackers from accessing their consumer reports; and/or failing to take reasonable security measures that would prevent unauthorized entities or computer hackers from accessing their consumer reports.

66. The Federal Trade Commission ("FTC") has pursued enforcement actions against consumer reporting agencies under the FCRA for failing to "take adequate measures to fulfill their obligations to protect information contained in consumer reports, as required by the" FCRA, in connection with data breaches.

67. Equifax willfully and/or recklessly violated § 1681b and § 1681e(a) by providing impermissible access to consumer reports and by failing to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under section 1681b of the FCRA. The willful and reckless nature of Equifax's violations is supported by, among other things, former employees' admissions that Equifax's data security practices have deteriorated in recent years, and Equifax's numerous other data breaches in the past. Further, Equifax touts itself as an industry leader in breach prevention; thus, Equifax was well aware of the importance of the measures organizations should take to prevent data breaches, and willingly failed to take them.

68. Equifax also acted willfully and recklessly because it knew or should have known about its legal obligations regarding data security and data breaches under the FCRA. These obligations are well established in the plain language of the FCRA and in the promulgations of the Federal Trade Commission. See, e.g., 55 Fed. Reg. 18804 (May 4, 1990), 1990 Commentary On The Fair Credit Reporting Act. 16 C.F.R. Part 600, Appendix To Part 600, Sec. 607 2E. Equifax obtained or had available these and other substantial written materials that apprised them of their duties under the FCRA. Any reasonable consumer reporting agency knows or should know about these requirements. Despite knowing of these legal obligations, Equifax acted consciously in breaching known duties regarding data security and data breaches and depriving Plaintiffs and other members of the Classes of their rights under the FCRA.

69. Equifax's willful and/or reckless conduct provided a means for unauthorized intruders to obtain and misuse Plaintiffs' and the Class Members' PII for no permissible purposes under the FCRA.

70. Plaintiffs and the Class Members have been damaged by Equifax's willful or reckless failure to comply with the FCRA. Therefore, Plaintiffs and each of the Class Members are entitled to recover "any actual damages sustained by the consumer . . . or damages of not less than $100 and not more than $1,000." 15 U.S.C. § 1681n(a)(1)(A).

71. Plaintiffs and the Class Members are also entitled to punitive damages, costs of the action, and reasonable attorneys' fees. 15 U.S.C. § 1681n(a)(2) & (3).

COUNT II

NEGLIGENT VIOLATION OF THE FAIR CREDIT REPORTING ACT

72. Plaintiffs incorporate paragraphs 1 through 71 by reference.

73. Equifax was negligent in failing to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under section 1681b of the FCRA. Equifax's negligent failure to maintain reasonable procedures is supported by, among other things, former employees' admissions that Equifax's data security practices have deteriorated in recent years, and Equifax's numerous other data breaches in the past. Further, as an enterprise claiming to be an industry leader in data breach prevention, Equifax was well aware of the importance of the measures organizations should take to prevent data breaches, yet failed to take them.

74. Equifax's negligent conduct provided a means for unauthorized intruders to obtain Plaintiffs' and Class Members' PII and consumer reports for no permissible purposes under the FCRA.

75. Plaintiffs and the Class Members have been damaged by Equifax's negligent failure to comply with the FCRA. Therefore, Plaintiffs and each of the Class Members are entitled to recover "any actual damages sustained by the consumer." 15 U.S.C. § 1681o(a)(1).

76. Plaintiffs and the Class Members are also entitled to recover their costs of the action, as well as reasonable attorneys' fees. 15 U.S.C. § 1681o(a)(2).

COUNT III

NEGLIGENCE

77. Plaintiffs incorporate paragraphs 1 through 76 by reference.

78. Equifax owed a duty to Plaintiffs and Class Members to exercise reasonable care in safeguarding their sensitive personal information. This duty included, among other things, designing, maintaining, monitoring, and testing Equifax's security systems, protocols, and practices to ensure that Class Members' information was adequately secured from unauthorized access.

79. Equifax owed a duty to Class Members to implement intrusion detection processes that would detect a data breach in a timely manner.

80. Equifax also had a duty to delete any PII that was no longer needed to serve client needs.

81. Equifax owed a duty to disclose the material fact that its data security practices were inadequate to safeguard Class Members' PII.

82. Equifax also had independent duties under state laws that required Equifax to reasonably safeguard Plaintiffs' and Class Members' PII and promptly notify them about the Data Breach.

83. Equifax had a special relationship with Plaintiffs and Class Members because the Plaintiffs and Class Members entrusted Equifax with their PII. This provided an independent duty of care. Moreover, Equifax had the ability to protect its systems and the PII it stored on them from attack.

84. Equifax breached its duties by, among other things: (a) failing to implement and maintain adequate data security practices to safeguard Class Members' PII; (b) failing to detect and end the Data Breach in a timely manner; (c) failing to disclose that Defendants' data security practices were inadequate to safeguard Class Members' PII; and (d) failing to provide adequate and timely notice of the breach.

85. Because of Equifax's breach of its duties, Class Members' PII has been accessed by unauthorized individuals.

86. Plaintiffs and Class Members were foreseeable victims of Equifax's inadequate data security practices. Equifax knew or should have known that a breach of its data security systems would cause damages to Class Members.

87. Equifax engaged in this misconduct recklessly, in conscious neglect of duty and in callous indifference to consequences, and, in the alternative, with such want of care as would raise a presumption of a conscious indifference to consequences. Equifax was, or should reasonably have been, aware of its misconduct and of the foreseeable injury that would probably result, and with reckless indifference to consequences, consciously and intentionally committed the wrongful acts and omissions herein. Equifax's actions and omissions were, therefore, not just negligent, but grossly negligent, reckless, willful, and wanton.

88. As a result of Equifax's negligence, Plaintiffs and Class Members suffered and will continue to suffer injury, which includes but is not limited to the monetary difference

between the amount paid for services as promised and the services actually provided by Defendants (which did not include adequate or industry standard data protection), inconvenience and exposure to a heightened, imminent risk of fraud, identity theft, and financial harm. Plaintiffs and Class Members must more closely monitor their financial accounts and credit histories to guard against identity theft. Class Members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The unauthorized acquisition of Plaintiffs' and Class Members' PII has also diminished the value of the PII. Plaintiffs and the Class Members have also experienced other damages consistent with the theft of their PII. Through its failure to timely discover and provide clear notification of the Data Breach to consumers, Equifax prevented Plaintiffs and Class Members from taking meaningful, proactive steps to secure their PII.

89. The damages to Plaintiffs and the Class Members were a direct, proximate, reasonably foreseeable result of Equifax's breaches of its duties.

90. Therefore, Plaintiffs and Class Members are entitled to damages in an amount to be proven at trial.

COUNT IV

NEGLIGENCE PER SE

91. Plaintiffs incorporate paragraphs 1 through 90 by reference.

92. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Equifax, of failing to use reasonable measures to protect PII.

93. Equifax violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Equifax's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of a data breach at a corporation such as Equifax, including, specifically, the immense damages that would result to Plaintiffs and Class Members.

94. Equifax's violation of Section 5 of the FTC Act constitutes negligence per se.

95. Equifax also violated the FCRA, as stated in Counts I and II. Equifax's violation of the FCRA constitutes negligence per se.

96. The Gramm-Leach-Bliley Act ("GLBA") requires covered entities to satisfy certain standards relating to administrative, technical, and physical safeguards:

> (1) to insure the security and confidentiality of customer records and information;
>
> (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and
>
> (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.
>
> 15 U.S.C. § 6801(b).

97. Businesses subject to the GLBA "should take preventative measures to safeguard customer information against attempts to gain unauthorized access to the information." Interagency Guidelines Establishing Information Security Standards, 12 C.F.R. pt. 225, App. F.

98. In order to satisfy their obligations under the GLBA, Equifax was required to "develop, implement, and maintain a comprehensive information security program that is [1] written in one or more readily accessible parts and [2] contains administrative, technical, and physical safeguards that are appropriate to [its] size and complexity, the nature and scope of [its]

activities, and the sensitivity of any customer information at issue." See 16 C.F.R. § 314.3; *see also* Interagency Guidelines Establishing Information Security Standards, 12 C.F.R. pt. 225, App. F. (Subject companies must "design its information security program to control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of the [...] company's activities"). This obligation included considering and, where the Company determined appropriate, adopting mechanisms for "[e]ncryption of electronic customer information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access." *Id.*

99. In addition, under the Interagency Guidelines Establishing Information Security Standards, 12 C.F.R. pt. 225, App. F., Equifax had an affirmative duty to "develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems." *See id.* "The program should be appropriate to the size and complexity of the institution and the nature and scope of its activities." *Id.*

100. Equifax had an "affirmative duty to protect their customers' information against unauthorized access or use." *Id.* Timely notification of customers in the event of a data breach is key to meeting this affirmative obligation. Accordingly, when Equifax became aware of "unauthorized access to sensitive customer information," it should have "conduct[ed] a reasonable investigation to promptly determine the likelihood that the information has been or will be misused" and "notif[ied] the affected customer[s] as soon as possible." *See id.* Sensitive customer information includes much of the PII released in the Data Breach.

101. Equifax violated the GLBA by failing to "develop, implement, and maintain a comprehensive information security program" with "administrative, technical, and physical

safeguards" that were "appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue." This includes, but is not limited to, Equifax's (a) failure to implement and maintain adequate data security practices to safeguard Class Members' PII; (b) failure to detect the Data Breach in a timely manner; and (c) failure to disclose that Defendants' data security practices were inadequate to safeguard Class Members' PII.

102. Equifax also violated the GLBA by failing to notify affected customers as soon as possible after it became aware of unauthorized access to sensitive customer information.

103. Equifax's violations of the GLBA constitute negligence per se.

104. Plaintiffs and Class Members are within the class of persons that the FTC Act, the FCRA, and the GLBA were intended to protect.

105. Plaintiffs and Class Members were foreseeable victims of Equifax's violation of the FTC Act, the FCRA, and the GLBA. Equifax knew or should have known that its failure to take reasonable measures to prevent a breach of its data security systems, and failure to timely and adequately report it to Class Members themselves would cause damages to Class Members.

106. The harm that occurred as a result of the Equifax Data Breach is the type of harm the FTC Act, the FCRA, and the GLBA were intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

107. Equifax engaged in this misconduct recklessly, in conscious neglect of duty and in callous indifference to consequences, and, in the alternative, with such want of care as would raise a presumption of a conscious indifference to consequences. Equifax was or should

reasonably have been, aware of its misconduct and of the foreseeable injury that would probably result, and with reckless indifference to consequences, consciously and intentionally committed the wrongful acts and omissions herein. Equifax's actions and omissions were, therefore, not just negligent, but grossly negligent, reckless, willful, and wanton.

108. As a direct and proximate result of Equifax's negligence *per se*, Plaintiffs and Class Members suffered and will continue to suffer injury, which includes but is not limited to the monetary difference between the amount paid for services as promised and the services actually provided by Defendants (which did not include adequate or industry standard data protection), inconvenience and exposure to a heightened, imminent risk of fraud, identity theft, and financial harm. Plaintiffs and Class Members must more closely monitor their financial accounts and credit histories to guard against identity theft. Class Members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The unauthorized acquisition of Plaintiffs' and Class Members' PII has also diminished the value of the PII. Plaintiffs and the Class Members have also experienced other damages consistent with the theft of their PII. Through its failure to timely discover and provide clear notification of the Data Breach to consumers, Equifax prevented Plaintiffs and Class Members from taking meaningful, proactive steps to secure their PII.

109. But for Equifax's violation of the applicable laws and regulations, Class Members' PII would not have been accessed by unauthorized individuals.

110. The damages to Plaintiffs and the Class Members were a direct, proximate, reasonably foreseeable result of Equifax's breaches of the applicable laws and regulations.

111. Therefore, Plaintiffs and Class Members are entitled to damages in an amount to be proven at trial.

COUNT V

UNJUST ENRICHMENT

112. Plaintiffs incorporate paragraphs 1 through 111 by reference.

113. Equifax received payment to perform services that included protecting Plaintiffs' and the Class Members' PII. Equifax failed to do this, but retained Plaintiffs' and the Class Members' payments.

114. Equifax retained the benefit of said payments under circumstances which renders it inequitable and unjust for it to retain such benefits without paying for their value.

115. Defendants have knowledge of said benefits.

116. Plaintiffs and Class Members are entitled to recover damages in an amount to be proven at trial.

COUNT VI

INVASION OF PRIVACY- PUBLIC DISCLOSURE OF PRIVATE FACTS

117. Plaintiffs incorporate paragraphs 1 through 116 by reference.

118. Plaintiffs' and the Class Members' PII is private, highly sensitive information. Dissemination of one's PII to data hackers and to the public would be substantially and highly offensive to a reasonable person.

119. The public has no legitimate interest in Plaintiffs' and the Class Members' PII, and Plaintiffs and the Class Members have a legally protectable interest in their PII.

120. Equifax publicly disclosed and disseminated Plaintiffs' and the Class Members' PII. Equifax willfully failed to safeguard and protect Plaintiffs' and the Class Members' PII --

including by failing to take adequate corrective measures once the data breach occurred. Equifax's actions directly and proximately resulted in unreasonable publicity to the private lives of Plaintiffs and the Class Members and deprived them of their legal interest in the privacy of their PII.

121. As a result, Plaintiffs and the Class Members have suffered and continue to suffer substantial injury and damages.

COUNT VII

BAILMENT

122. Plaintiffs incorporate paragraphs 1 through 121 by reference.

123. Plaintiffs and Class Members delivered their PII to Defendants in order to receive services from Defendants.

124. The PII was furnished to Defendants for the exclusive purpose of receiving the services Equifax provides in the ordinary course of business, and Defendants took possession of the PII for the same reason.

125. Upon delivery, Plaintiffs and Class Members intended and understood that Equifax would adequately safeguard their PII, and Defendants, in accepting possession, understood the expectations of Plaintiffs and Class Members. Accordingly, bailment was established for the mutual benefit of the parties at the time of delivery and acceptance of possession.

126. Pursuant to the bailment arrangement, Defendants owed Plaintiffs and Class Members a duty of reasonable care in safeguarding and protecting their PII.

127. Equifax breached this duty by failing to take adequate steps to protect the PII entrusted to them and by failing to conform to best practices and industry standards to prevent unauthorized access to Plaintiffs and Class members' PII.

128. As a result of Equifax's failure to fulfill its bailment arrangement, Plaintiffs and Class Members suffered and will continue to suffer injury, which includes but is not limited to the monetary difference between the amount paid for services as promised and the services actually provided by Defendants (which did not include adequate or industry standard data protection), inconvenience and exposure to a heightened, imminent risk of fraud, identity theft, and financial harm. Plaintiffs and Class Members must more closely monitor their financial accounts and credit histories to guard against identity theft. Class Members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The unauthorized acquisition of Plaintiffs' and Class Members' PII also has diminished the value of the PII. Through its failure to timely discover and provide clear notification of the Data Breach to consumers, Equifax prevented Plaintiffs and Class Members from taking meaningful, proactive steps to secure their PII.

COUNT VIII

DECLARATORY JUDGMENT

129. Plaintiffs incorporate paragraphs 1 through 128 by reference.

130. Equifax owes duties of care to Plaintiffs and Class Members that require it to adequately secure PII.

131. Equifax still possesses PII pertaining to Plaintiffs and Class Members.

132. Equifax has made no announcement or notification that it has remedied the vulnerabilities in its computer data systems, and, most importantly, its systems.

133. Accordingly, Equifax has not satisfied its contractual obligations and legal duties to Plaintiffs and Class Members. In fact, now that Equifax's lax approach towards data security has become public, the PII in its possession is more vulnerable than previously.

134. Equifax's breach of its contractual obligations and duties of care caused Plaintiffs and Class Members actual harm.

135. Plaintiffs, therefore, seek a declaration that (a) Equifax's existing data security measures do not comply with its contractual obligations and duties of care, and (b) in order to comply with its contractual obligations and duties of care, Equifax must implement and maintain reasonable security measures, including, but not limited to:

a. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Equifax's systems on a periodic basis, and ordering Equifax to promptly correct any problems or issues detected by such third-party security auditors;

b. engaging third-party security auditors and internal personnel to run automated security monitoring;

c. auditing, testing, and training its security personnel regarding any new or modified procedures;

d. segmenting PII by, among other things, creating firewalls and access controls so that if one area of Equifax is compromised, hackers cannot gain access to other portions of Equifax systems;

e. purging, deleting, and destroying in a reasonable secure manner PII not necessary for its provisions of services;

f. conducting regular database scanning and securing checks;

g. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. educating its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Equifax customers must take to protect themselves.

PRAYER FOR RELIEF ON INDIVIDUAL AND CLASS ACTION CLAIMS

WHEREFORE, the Plaintiffs and Class Representatives, on their own behalf and on behalf of the Class, pray that this Court:

(1) Certify this case as a class action maintainable under Federal Rules of Civil Procedure Rule 23, on behalf of the proposed Class; designate the Plaintiffs as Class Representatives; and designate Plaintiffs' counsel of record as Class Counsel;

(2) Declare and adjudge that Defendants' policies, practices, and procedures challenged herein are illegal and in violation of the rights of the Plaintiffs and Class Members;

(3) Issue a permanent injunction against Defendants and their partners, officers, trustees, owners, employees, agents, attorneys, successors, assigns, representatives, and any and all persons acting in concert with them from engaging in any conduct violating the rights of Plaintiffs, members of the Class, and those similarly situated to them;

(4) Order injunctive relief requiring Defendants to (a) strengthen their data security systems that maintain PII to comply with the applicable state laws alleged herein and best practices under industry standards; (b) engage third-party auditors and internal personnel to conduct security testing and audits on Defendants' systems on a periodic

basis; (c) promptly correct any problems or issues detected by such audits and testing; and (d) routinely and continually conduct training to inform internal security personnel how to prevent, identify and contain a breach, and how to appropriately respond;

(5) Award compensatory, consequential, incidental, and statutory damages, restitution, and disgorgement to Plaintiffs and Class Members in an amount to be determined at trial;

(6) Order Defendants to make the Plaintiffs and Class Members whole by providing them with any other monetary and affirmative relief;

(7) Order Defendants to pay all costs associated with Class notice and administration of Class-wide relief;

(8) Award Plaintiffs and the Class their litigation costs and expenses, including, but not limited to, reasonable attorneys' fees;

(9) Award Plaintiffs and Class Members all pre-judgment interest and post-judgment interest available under law;

(10) Award Plaintiffs and Class Members any other appropriate equitable relief;

(11) Order that this Court retain jurisdiction of this action until such time as the Court is satisfied that the Defendants have remedied the practices complained of herein and are determined to be in full compliance with the law; and

(12) Award additional and further relief as this Court may deem just and proper.

JURY DEMAND

Plaintiffs demand a trial by jury on all issues triable of right by jury.

/s/ Amber Griffin Shaw
Amber Shaw (MS Bar # 103039)
GORDON SHAW LAW GROUP, PLLC
114 West Liberty Street, Suite 300
P.O. Box 846
Covington, TN 38019
Telephone: (901) 476-7100
Facsimile: (901) 476-3537
ashaw@lawjhg.com

*Kevin Sharp (TN Bar #16287)
SANFORD HEISLER SHARP, LLP
611 Commerce St., Suite 3100
Nashville, TN 37203
Telephone: (615) 434-7001
Facsimile: (615) 434-7020
ksharp@sanfordheisler.com

**seeking admission pro hac vice*

Attorney for Plaintiff and the Class